UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/591,786	09/05/2006	Sebastien Canard	33901-220PUS	4281

7590 10/16/2008

Thomas Langer
Cohen Pontani Lieberman & Pavane
Suite 1210
551 fifth Avenue
New York, NY 10176

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/591,786	CANARD ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☒ Claim(s) *12-18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/5/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the original filing of September 5, 2006. Claims (1-18) are pending.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). This application is a 371 of PCT/EP05/02162 filed on 2/28/2005 and further claim foreign priority to EUROPEAN PATENT OFFIC (EPO) 04290557.0 filed on 3/2/2004.

Claim Objections

2. Claims 10-18 are objected to because of the following informalities: Claims contain numeric reference, **"Voter Module (10)"** for which should not be part of the claim limitation. Applicant is advised to delete such numeric references. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 12, 14, 16, and 18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim is directed to a computer product for which is non-statutory subject matter. The recitation of the intended use of the computer program product on a computer having a computer readable medium does not require the computer program product to be encoded on a computer-readable medium. Accordingly, the scope of the claims includes the computer program product by itself, which is function descriptive material and does not fall into at least one of the four statutory classes defined by 35 U.S.C. 101. The computer program product, only imparts functionality when employed as a computer component, such as when a computer program is recorded on a computer readable medium.

Applicant is advised to amend claims 12, 14, 16, and 18 to read, " a computer program executing on a processor which, when used on a computer apparatus", to overcome 101 rejection.

4. Claim 10 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim is directed to a system for which is indicative of software. As such, the claim recites non-statutory subject matter.

Applicant is advised to amend claims 10 to read, " a electronic voting system comprising: a processor ..." to overcome 101 rejection.

5. Claim 11 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim is directed to a voter module for which is indicative of software. As such, the claim recites non-statutory subject matter.

Applicant is advised to amend claim 11 to read, " ... comprising a processor, and the voter's vote", to overcome 101 rejection.

6. Claim 13 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim is directed to a voting system admin server module for which is indicative of software. As such, the claim recites non-statutory subject matter.

Applicant is advised to amend claim 13 to read, " ... comprising a processor, and the voter's vote", to overcome 101 rejection.

7. Claim 15 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim is directed to a voting system randomizer module for which is indicative of software. As such, the claim recites non-statutory subject matter.

Applicant is advised to amend claim 15 to read, "A voting system randomizer module comprising a processor ....", to overcome 101 rejection.

8. Claim 17 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim is directed to a voting system tallier

module for which is indicative of software. As such, the claim recites non-statutory subject matter.

Applicant is advised to amend claim 17 to read, "A voting system trallier module comprising a processor ....", to overcome 101 rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Fujioka et al. (US Patent No. 6,845,447 and Fujioka hereinafter).

10. As to claim 1, Fujioka teaches a **electronic voting method comprising the step of using a fair blind signature scheme to obtain a digital signature (Yi) of a data signal (xi) comprising a voter's vote (I~i))** (i.e., ... teaches A voter V.sub.i encrypts his vote content v.sub.i with a public key k.sub.PC of a counter C, then concatenates the encrypted vote content x.sub.i with a tag t.sub.i to obtain a ballot z.sub.i, then randomizes it with a random number r.sub.i to create a preprocessed text

e.sub.i, and sends it and a signature s.sub.i therefor to an election administrator A. … teaches a administrator A generates a blind signature d.sub.i for the preprocessed text e.sub.i and sends it back to the voter V.sub.i. … teaches a voter V.sub.i excludes the influence of the random number r.sub.i from the blind signature d.sub.i to obtain administrator signature y.sub.i, and sends vote data <z.sub.i, y.sub.i > to a counter C.[abstract].

11. As to claim 2, Fujioka teaches a **electronic voting where the fair blind signature scheme is a threshold fair blind signature scheme in which the digital signature is obtained from a sub-set of a group of servers, the group of servers containing n servers and the sub-set containing t servers, where t n** (i.e., … teaches the decryption process involves the use of a distributed secret key k.sub.SCj of every distributed counter, or requires a certain number (a threshold value U.sub.t (where 2<U.sub.t <U) of people to work together [col. 9, lines 20-26]).

12. As to claim 3, Fujioka teaches a **electronic voting method where the data signal (xi) corresponds to the voter's vote (v/) encrypted according to a first encryption scheme (ErM)** (i.e., … teaches A voter V.sub.i encrypts his vote content v.sub.i with a public key k.sub.PC [abstract]), said first encryption scheme being the encryption scheme of a first mix-net **(TM)**, and the method further comprises the step of applying the decryption scheme **(DrM)** inverse to said first encryption scheme to said data signal (xi) whereby to retrieve the voter's vote (vi).

13. As to claim 4, Fujioka teaches a **electronic voting method comprising the steps of:**

receiving, in a first order, a batch of encrypted data signals, each encrypted data signal (ci) comprising data encrypted according to a second encryption scheme (EM) said data including a respective data signal (xl) [abstract];

retrieving each data signal (xl) from the respective encrypted data signal (ci) in said batch by applying a decryption scheme (DM) inverse to said second encryption scheme (EM) (i.e., ... teaches the encrypted vote are decrypted [col. 3, lines 10-20])**;**

and outputting the retrieved data signals (xl) for said batch in a different order from said first order [fig, 3].

14. As to claim 5, Fujioka teaches a **electronic voting method where said second encryption scheme is the encryption scheme of a second mix-net (M)** [abstract].

15. As to claim 6, Fujioka teaches a **electronic voting method comprising the step of detecting irregularities in the voting process, said step of detecting irregularities comprising verifying that the ballots to be counted do not contain duplicated data-pairs** (i.e., ... teaches and makes a check in the list checking part 170 to see if the number of ballots placed on the ballot list 320A is equal to the number of

voters published [col. 8, lines 20-30]), **wherein a data-pair corresponds to one of said data signals and the digital signature thereof** [fig. 6].

16. As to claim 7, Fujioka teaches a **electronic voting method comprising the step of detecting irregularities in the voting process, wherein the step of detecting irregularities comprises checking the validity of the digital signatures in the ballots to be counted** (i.e., .. teaches checking the verification of the digital signatures compliance to equation [col. 8, lines 1-10]).

17. As to claim 8, Fujioka teaches a **electronic voting method and comprising the step of detecting irregularities in the voting process, wherein the step of detecting irregularities comprises checking that there is no overlap between the ballots to be counted and entries in a revocation list** (i.e., … teaches verifying if the voter is eligible to vote [col. 7, lines 9-25]).

18. As to claim 9, Fujioka teaches a **electronic voting method claim and comprising the steps of:**

receiving said data signal (xi) for digital signature according to said fair blind signature scheme at a server module (AS), said data signal (xi) comprising a vote (vi) selected by a voter (VI), said vote (vi) being encrypted according to said first encryption scheme (ETM), blinded according to said fair blind signature

scheme and digitally signed according to a digital signature scheme of said voter [abstract];

verifying, by said server module (AS), that the digital signature (si) in the received signal is valid (i.e., .. teaches checking the verification of the digital signatures compliance to equation [col. 8, lines 1-10])**;**

in the case where the verifying step confirms that the digital signature in the signal received by said server module (AS) is valid, said server module (AS) digitally signs the blinded encrypted vote (el) and outputs the digitally-signed message (SAs(ei)) [abstract]**;**

unblinding the digitally-signed message (SAs(ei)) to yield said digital signature (3/) of the data signal (xi) [abstract]**;**

encrypting said data signal (xi) and said digital signature (Yi) thereof according to said second encryption scheme (EM) to produce encrypted data signal (cl) (i.e., … teaches each voter encrypts his vote content by a public key of the counter, then randomizes the encrypted vote content by a random number to create a preprocessed text, then attaches thereto his signature, and sends the signed text to the election administrator [col. 2, lines 33-40])**;**

and signing said encrypted data signal according to a signature scheme of the voter (Vi) [abstract]**.**

19. As to claim 10, Fujioka teaches a **electronic voting system comprising: a plurality of voter modules (10), and an admin server module (20), wherein a voter**

module (10) and the admin server module (20) cooperate in application of a fair blind signature scheme whereby to obtain a digital signature 0'i) of a data signal (xi) comprising the respective voter's vote (vi) [abstract].

20. As to claim 11, Fujioka teaches a **voter module (10) adapted to cooperate with an admin server module (20) in application of a fair blind signature scheme whereby to obtain a digital signature (yl) of a data signal (xi) comprising the voter's vote (vi**) [abstract].

21. As to claim 12, Fujioka teaches a **computer program having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voter module (10) according to claim 11** [col. 2, lines 29-32].

22. As to claim 13, Fujioka teaches a **voting system admin server module (20) adapted to cooperate with a voter module (10) in application of a fair blind signature scheme whereby to obtain a digital signature 0'i) of a data signal (xi) comprising the voter's vote (vl)** (i.e., ... teaches A voter V.sub.i encrypts his vote content v.sub.i with a public key k.sub.PC of a counter C, then concatenates the encrypted vote content x.sub.i with a tag t.sub.i to obtain a ballot z.sub.i, then randomizes it with a random number r.sub.i to create a preprocessed text e.sub.i, and sends it and a signature s.sub.i therefor to an election administrator A. … teaches a

administrator A generates a blind signature d.sub.i for the preprocessed text e.sub.i and sends it back to the voter V.sub.i. ... teaches a voter V.sub.i excludes the influence of the random number r.sub.i from the blind signature d.sub.i to obtain administrator signature y.sub.i, and sends vote data <z.sub.i, y.sub.i > to a counter C.[abstract]).

23. As to claim 14, Fujioka teaches a **computer program having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system admin server module (20) according to claim 13** (i.e., ... teaches election administrator verifies the validity of the voter through utilization of his signature attached to the encrypted text [col. 2, lines 35-40].

24. As to claim 15, Fujioka teaches a **voting system randomizer module (40) comprising: input means for receiving a batch of cast votes, each cast vote comprising an encrypted data signal (cl) comprising a respective voter's vote (vi) digitally signed according to a fair blind signature scheme** [abstract], **each encrypted data signal (cl) being encrypted according to a predetermined encryption scheme (EM)** (i.e., ... teaches each voter encrypts his vote content by a public key of the counter, then randomizes the encrypted vote content by a random number to create a preprocessed text, then attaches thereto his signature, and sends the signed text to the election administrator [col. 2, lines 33-40]);

and a mix-net (Mr) for decrypting said encrypted data signals (ci) by applying a decryption scheme (DM) inverse to said predetermined encryption scheme (EM) (i.e., ... teaches the encrypted vote are decrypted [col. 3, lines 10-20]);

and output means for outputting the decrypted signals of said batch in an order different from the order of the corresponding encrypted data signals in said batch [fig. 3].

25. As to claim 16, Fujioka teaches a **computer program having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system randomizer module (40) according to claim 15** (i.e. , ... teaches a randomizer [fig. 3]).

26. As to claim 17, Fujioka teaches a **voting system tallier module (50) comprising: input means for receiving cast votes** [fig. 7], **each cast vote comprising a data signal (x~) digitally signed according to a fair blind signature scheme** (i.e., ... teaches a blind signature [abstract]), **each data signal (xi) comprising a respective voter's vote (vi) encrypted according to an encryption scheme (ErM)** (i.e., ... teaches encrypted vote content [abstract]);

and a mix-net (M) for decrypting said encrypted votes (vi) by applying a decryption scheme (DrM) inverse to said encryption scheme (ErM) (i.e., ... teaches the encrypted vote are decrypted [col. 3, lines 10-20]).

27. As to claim 18, Fujioka teaches a **computer program having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system tallier module (50)** (i.e., ... teaches a counter apparatus [fig. 7]).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431